Un Proceso Práctico de Análisis de Riesgos de Activos de Información

Mg. Marcos Sotelo Bedón [1,2], José Torres Utrilla[3], Juan Rivera Ortega[4]
Marcos.sotelo@bcrp.gob.pe, jdtorresu@uni.pe, river.rbk@gmail.com

[1]Gerencia de Tecnologías de Información, Banco Central de Reserva de Perú (BCRP)
[2]Universidad Nacional Mayor de San Marcos (UNMSM)
[3]Universidad Nacional de Ingeniería (UNI)
[4]Universidad de San Martin de Porres (USMP)

Resumen: *El artículo presenta un proceso de análisis de riesgos de activos de información, en el contexto de un Sistema de Gestión de Seguridad de Información (SGSI) alineado al estándar ISO/IEC 27001:2005 y un software (prototipo) que le brinda soporte, aunado a un portal cuyo contenido tiene por finalidad sensibilizar en gestión de riesgos y seguridad de información. Este proceso sigue los lineamientos de los principales estándares y buenas prácticas en gestión de riesgos y seguridad de la información, y viene siendo aplicado en el país en los últimos cinco años. El presente proceso utiliza el marco referencial Magerit (Metodología de Análisis y Gestión de Riesgos de Tecnologías de Información) como eje de la propuesta, no obstante cabe mencionar que a diferencia de este marco, el proceso en mención incorpora el Análisis de Impacto de Negocio(BIA), el cual tiene por objetivo evaluar el impacto sobre los procesos de negocio, debido a la no disponibilidad de los servicios de tecnologías de información, lo que posteriormente se deriva en la obtención del nivel de criticidad para cada activo de información, lo cual es indispensable para establecer el nivel de riesgo de los mismos.*

Abstract: *The article presents a process of risk analysis of information assets, in the context of a System of Information Security Management (ISMS) aligned to ISO / IEC 27001:2005, and software (prototype) that supports it. This process follows the guidelines of the major standards and best practices in risk management and information security, and has been applied in the country over the past five years, this process uses the frame of reference Magerit (Handbook of Risk Management Information Technology) as the core of the proposal, however it is noteworthy that unlike this framework, the process in question incorporates the Business Impact Analysis (BIA), which aims to assess the impact on business processes, due to the unavailability of information technology services, which subsequently leads to obtaining the level of criticality for each information asset, which is essential to establish the level of risk for them.*

Palabras clave: Gestión de riesgos; análisis de riesgos de activos de información; gestión de seguridad de la información; activos de información.

1. Introducción

La incorporación acelerada de las tecnologías de información en las entidades privadas y públicas ha dado paso a nuevos retos, siendo uno de los relevantes la gestión de la seguridad de sus activos de información, toda vez que son críticos para su competitividad o supervivencia [1]. En una gestión por procesos, las organizaciones son representadas por un conjunto de procesos (estratégicos, tácticos y operativos), los cuales son asistidos por diversos activos de información, tales como los Servicios TI, constituidos por un conjunto de activos TI, como se aprecia en la Figura 1.

En estos procesos, la información es uno de los recursos más importantes, por lo que su gestión eficiente constituye un factor crítico para el desempeño empresarial, debido a ello, requiere una adecuada protección. Una estrategia para darle esa protección es implantando un sistema de gestión de seguridad de información (SGSI), alineado al estándar ISO/IEC 27001 [2], es decir, un proceso sistemático, documentado y conocido por toda la organización. Para el éxito de estos proyectos es fundamental la participación de la alta dirección y el desarrollo de una cultura de seguridad de la información [3].

En muchas organizaciones existe un compromiso intrínseco de implantar un sistema SGSI. En el caso del sector público, la reciente aprobación de la Norma Técnico Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad.

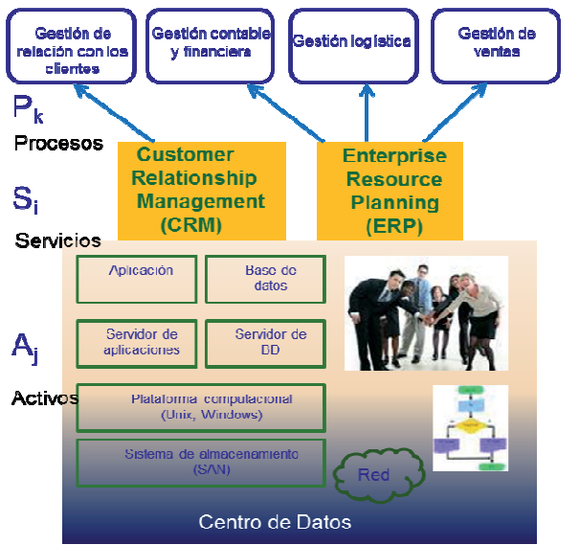

Figura 1. Procesos asistidos por Servicios TI. Fuente: Elaboración propia.

Sistemas de Gestión de Seguridad de la Información. Requisitos" mediante la Resolución Ministerial N° 129-2012-PCM [4] establece su implementación obligatoria en las Instituciones Públicas, siendo la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) el

organismo encargado de supervisar dicha implementación; ello origina la disyuntiva de cómo iniciar un proceso que permita su implementación exitosa. Es en este contexto que surge la propuesta, el cual pretende contribuir en la solución de dicho problema, a través de la descripción de un proceso de análisis de riesgos de activos de información.

En líneas generales, implantar un SGSI comprende los procesos o actividades ilustradas en la Figura 2, que pueden descomponerse en:

1. Identificar los objetivos del negocio.
2. Obtener el patrocinio de la alta dirección.
3. Establecer el alcance (algunos procesos del negocio).
4. Realizar un diagnóstico (Gap Analysis).
5. Asignar recursos y capacitar al equipo.
6. Analizar los riesgos de activos de información.
7. Elaborar y ejecutar un plan de tratamiento de riesgos.
8. Establecer la normativa para controlar el riesgo.
9. Monitorizar la implantación del SGSI.
10. Prepararse para la auditoría de certificación.
11. Llevar a cabo auditorías internas periódicas.

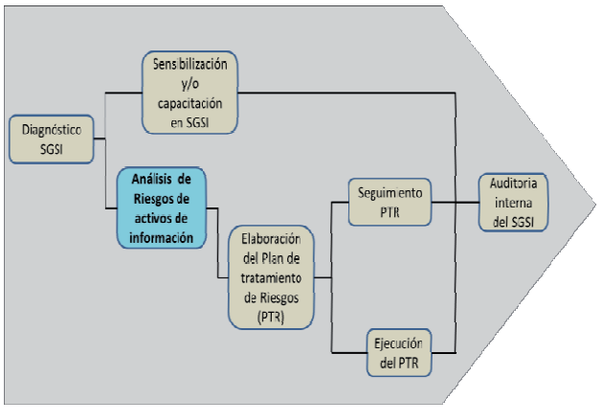

Figura 2. Actividades del SGSI. Fuente: Elaboración propia.

Siendo uno de los más relevantes el proceso de Análisis de Riesgos, que comprende la identificación, estimación y evaluación de riesgos. Es por ello que este artículo presenta un proceso de análisis de riesgos de activos de información y un software (prototipo) que lo asiste.

La estructura del artículo comienza con una breve introducción, en la cual se describe el problema y la propuesta de solución, consistente en la formulación de un proceso de Análisis de Riesgos de activos de Información. En la sección 2, se hace un recuento breve de trabajos relacionados y de los estándares de Gestión de Riesgos y Seguridad de Información, para luego pasar a detallar el proceso propuesto, continuando con el análisis de resultados y las posteriores conclusiones.

2. Trabajos Previos

En el contexto local, casi no existen publicaciones relacionadas con la propuesta. La mayoría de información concerniente al tema es abordada por los estándares y manuales de buenas prácticas en Gestión de Riesgos y seguridad de la información, sin embargo un estudio denominado ISRAM: Information security risk analysis method [5] brinda un enfoque cuantitativo de Análisis de Riesgos de Información.

La gestión integral de riesgos ha ganado impulso en los últimos años, especialmente a partir de la década de los noventa, lo que ha conllevado la aparición de "Modelos de Gestión de Riesgos", algunos de ellos de carácter general, como los estándares Australiano /neozelandés (AS/NZS 4630) e ISO/IEC 31000, y otros de carácter más específico, tales como: Commitee of Sponsoring Organizations (COSO), ISO 14000, ISO 22000, ISO 27005 y Occupational Health and Safety Advisory Services (OHSAS).

a. Estándar Australiano / neozelandés (AS/NZS 4360:2004)

El proceso de gestión de riesgos propuesto por la norma AS/NZS 4360:2004 [6] contempla los siguientes sub-procesos:

- Establecimiento del contexto.
- Identificación de riesgos.
- Análisis de riesgos.
- Evaluación de riesgos.
- Tratamiento de los riesgos.

b. ISO 31000:2009

Este estándar propone unas pautas genéricas sobre cómo gestionar los riesgos de forma sistemática y transparente. El enfoque está estructurado en tres elementos claves para una efectiva gestión de riesgos:

- Los principios para la gestión de riesgos.
- La estructura de soporte.
- El proceso de gestión de riesgos.

c. ISO/IEC 27005:2008

El estándar ISO/IEC 27005:2008, define las directrices para elaborar el proceso de análisis de riesgos. Éste forma parte de la familia ISO 27000, y sirve de complemento a las dos primeras normas de la familia, ISO/IEC 27001:2005 e ISO/IEC 27002:2005. La propuesta es similar al AS/NZS y contempla los siguientes sub-procesos:

- Establecimiento del contexto.
- Valoración de riesgos.
- Tratamiento de riesgos.
- Aceptación de riesgos.
- Comunicación de riesgos.
- Monitorización y revisión de riesgos.

d. Métodos de Análisis y Gestión de Riesgos de Tecnologías de Información (MAGERIT)

El método MAGERIT [7], desarrollado por el Consejo Superior de Administración Electrónica, y publicado por el Ministerio de Administraciones Públicas de España, comprende dos grandes procesos: El análisis de riesgos y la gestión de riesgos.

El **análisis de riesgos** permite determinar qué tiene la organización y qué podría pasar. Para ello toma en consideración los elementos ilustrados en la Figura 3.

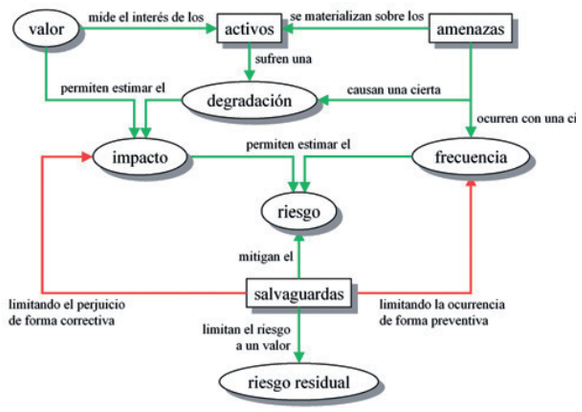

Figura 3. Elementos en el análisis de riesgos [7].

Los sub-procesos comprendidos son:

- Identificar los activos a tratar, las relaciones entre ellos y la valoración que merecen.
- Identificar las amenazas significativas sobre aquellos activos y valorarlos en términos de frecuencia de ocurrencia y degradación que causan sobre el valor del activo afectado.
- Identificar las salvaguardas existentes y se valorar la eficacia de su implementación.
- Estimar el impacto y el riesgo al que están expuestos los activos del sistema.
- Interpretar el significado del impacto y el riesgo.

La gestión de riesgos consiste en la estructuración de las acciones de seguridad para satisfacer las necesidades detectadas por el análisis. Comprende las actividades:

- Elegir una estrategia para mitigar el impacto y riesgo.
- Determinar las salvaguardas oportunas para el objetivo anterior.
- Determinar la calidad necesaria para dichas salvaguardas.
- Diseñar un plan de seguridad (plan de acción o plan director) para llevar el impacto y el riesgo a niveles aceptables.
- Llevar a cabo el plan de seguridad.

e. National Institute of Standards and Technology Special Publication (NIST SP 800-30): Guía de gestión de riesgos para sistemas de tecnologías de la información

El National Institute of Standards and Technology (NIST) ha dedicado una serie de publicaciones especiales a la seguridad de la información (SP 800). Esta serie incluye una metodología para el análisis y gestión de riesgos de seguridad de la información, NIST SP 800-30 [8], que comprende los siguientes subprocesos:

1. Caracterización de Sistemas.
2. Identificación de amenazas.
3. Identificación de vulnerabilidades.
4. Análisis de controles.
5. Determinación de probabilidades.
6. Análisis de impacto.
7. Determinación del riesgo.
8. Recomendación de controles.
9. Documentación de resultados.

3. Proceso propuesto

El proceso de análisis de riesgos de activos de información propuesto ha sido elaborado con base en su aplicación en una Institución del sector público, obteniéndose resultados satisfactorios, lo cual ha permitido su validación, haciendo a ésta factible de aplicar a las demás organizaciones del sector.

El proceso se definió siguiendo los lineamientos de los estándares descritos en la sección anterior, especialmente MAGERIT, donde la diferencia principal radica en la forma de determinación del impacto, que en este caso se hace a través del "Business Impact Analysis, BIA".

El proceso comprende, la identificación, estimación y evaluación de riesgos, como se ilustra en la Figura 4. Éste asume que el contexto está establecido, y se complementa con el tratamiento, monitorización y comunicación de riesgos, para completar la gestión de riesgos.

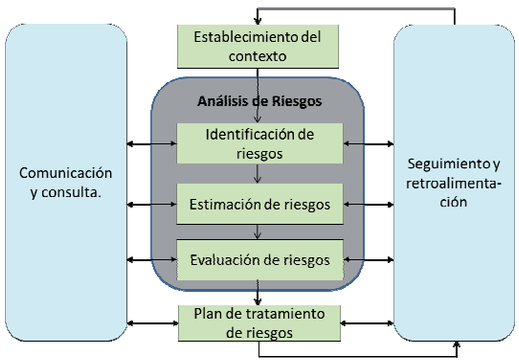

Figura 4. Análisis de riesgos de activos de información. Fuente: Adaptado del estándar ISO 31000:2009.

1. Establecimiento del contexto

El análisis de riesgos se realiza en el marco de la gestión integral del riesgo institucional. En el ámbito del SGSI el alcance del análisis de riesgos es el del SGSI, es decir, un conjunto de activos de información (A_i), que asisten a los procesos institucionales (P_k), que constituyen el alcance del SGSI.

En este proceso, el riesgo se determina en forma cualitativa, a partir de la Probabilidad, de que se materialice una amenaza, por el Impacto, que ocasione en la institución, a través de los procesos que asiste. La valoración de los dos factores se realiza con base en escalas de 5 valores, consignados en la Tabla 1 y Tabla 2. El riesgo resultante se clasifica en 4 niveles, como se ilustra en la Figura 5.

Nivel de aceptación o tolerancia al riesgo

Con base en el resultado del análisis de riesgos y lo consignado en la Tabla 3, los activos con riesgo extremo e intolerable deben ser llevados por lo menos al nivel tolerable, y aquellos activos críticos con nivel de riesgo tolerable deben ser llevados al nivel aceptable.

2. Identificación de riesgos

Comprende la identificación de los riesgos de los activos de información, por lo que demanda del inventario de estos activos [9], incluyendo su valor, determinado a partir de sus tres dimensiones de seguridad (Disponibilidad, Integridad y Confidencialidad) como mínimo. Para este proceso, los activos son agrupados en las categorías consignadas en la Tabla 4.

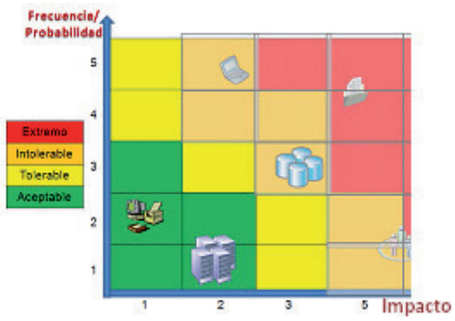

Figura 5. Mapa de riesgos. Fuente: Elaboración propia.

Probabilidad		
Valor	Grado	Descripción
1	Raro	Puede ocurrir una vez cada 2 años
2	Muy baja	Al año
3	Baja	En 6 meses
4	Media	Al mes
5	Alta	A la semana

Tabla 1. Valoración de la Probabilidad. Fuente: Elaboración propia.

Impacto		
Valor	*Nivel*	*Descripción*
1	Insignificante	Impacta levemente en la operatividad del proceso
2	Menor	Impacta en la operatividad del proceso
3	Moderado	Impacta en la operatividad del macro proceso
5	Mayor	Impacta en la operatividad de los procesos
8	Desastroso	Impacta fuertemente en la operatividad de los procesos

Tabla 2. Valoración del Impacto. Fuente: Elaboración propia.

Aceptación/Tolerancia		
Valor	*Nivel*	*Descripción*
1	Aceptable	Retenido
2	Tolerable	Para activos no críticos, pero intolerable para críticos
3	Intolerable	Atención inmediata y monitoreo permanente.
4	Extremo	Tratado como intolerable, pero a nivel de Gerencia General.

Tabla 3. Valoración del Nivel de Aceptación/Tolerancia. Fuente: Elaboración propia.

Categorías de Activos de Información		
Identificador	*Categoría*	*Ejemplos*
STI	Servicios TI	Aplicación + infraestructura TI de soporte.
SW	Software / Aplicaciones	Aplicaciones, sistemas operativos, herramientas de desarrollo y utilitarios
HW	Hardware / equipos	Servidores (S.O.), PCs, routers, hubs, firewalls, medio magnético, gabinetes, cajas fuertes, salas, mobiliario, sistema de alarma, etc.
SI	Soportes de información	SAN, discos, cintas, USB, CD, DVD.
COM	Redes de comunicaciones	Medios de transporte que llevan datos de un sitio a otro
DAT	Datos / Información	BD, archivos de datos, contratos y acuerdos, documentación del sistema, información de investigación, manuales de usuario, material de entrenamiento, de operación, procedimientos de soporte, planes de continuidad y contingencia, acuerdos
AUX	Equipamiento auxiliar	Equipamiento de soporte a los sistemas de información (UPS, Generados, Aire acondicionado, cableado, etc.)
INS	Locales / Instalaciones	Lugares donde se hospedan los sistemas de Información, registros vitales y comunicaciones
PER	Personal / RR.HH.	Personas, calificaciones, experiencia y capacidades (usuarios, proveedores, personal de TI)
SRV	Servicios generales	Vigilancia, servicios de impresión, computación, telecomunicaciones, eléctrica, agua, etc.

Tabla 4. Clasificación de Activos de Información. Fuente: Adaptado del estándar Magerit [7].

Los activos están expuestos a amenazas, que pueden materializarse (explotando vulnerabilidades) con determinada frecuencia o probabilidad, dependiendo de la eficacia de los controles o salvaguardas vigentes.

Para la determinación de riesgos, este proceso utiliza el catálogo de amenazas de MAGERIT, y las vulnerabilidades y controles identificados por los administradores de activos, con base en su experiencia e información de los fabricantes. Las amenazas están organizadas en las categorías consignadas en la Tabla 5, y pueden afectar a más de un tipo de activo.

Categorías de Amenazas	
Identificador	*Tipo*
N	Desastres naturales
I	De origen industrial
E	Errores y fallos no intencionados
A	Ataques intencionados

Tabla 5. Clasificación de las Amenazas. Fuente: Adaptado del estándar Magerit [7].

3. Estimación de riesgos

El equipo de análisis de riesgos (especialistas en riesgos, en seguridad, y administradores de activos) determina el impacto y probabilidad, calcula el riesgo actual, establece los controles recomendados, y determina el riesgo residual, es decir, el riesgo resultante luego de que se implementen los controles establecidos. El resultado es el Informe de Análisis de Riesgos, que establece el modo de tratamiento y los controles recomendados. El Riesgo de un servicio de información $\mathbf{S_i}$, denominado riesgo repercutido (RR) [2], es obtenido a partir de sus activos por medio de una función, tal como promedio (simple o ponderado) o máximo.

3.1. Determinación del Impacto

En este proceso, el impacto de un activo, $\mathbf{I(A_j)}$ es igual al impacto mayor de los servicios donde participa; a su vez, el impacto de un servicio $\mathbf{I(S_i)}$ es igual al impacto mayor de los procesos que asiste. El impacto de un proceso $\mathbf{I(P_k)}$ se determina en el proceso de análisis de impacto en el negocio (BIA - Business Impact Analysis).

El proceso BIA permite determinar el impacto de los procesos Pk, y la criticidad de los Servicios TI Si, que lo asisten. Asimismo, los tiempos de recuperación objetivo (RTO-Recovery Time Objective) y el impacto asociado con la interrupción de los procesos por un determinado periodo. Este proceso se realiza con la participación de los dueños de procesos.

El impacto de la interrupción de un proceso I(Pk), ocasionado por un incidente en uno de sus servicios Si, se determina a partir de tres (3) factores:

a) El impacto de su macroproceso en el cumplimiento de los objetivos de la entidad;

b) El nivel de dependencia del proceso $\mathbf{P_k}$, con relación a sus servicios $\mathbf{S_i}$.

c) El impacto del proceso $\mathbf{P_k}$ en función a los tiempos de recuperación objetivo (RTO-Recovery Time Objective).

Para el factor (a), los dueños de macroprocesos asignan un valor de impacto (Alto, Medio, Bajo) para cada macroproceso. Para el factor (b), utilizando la matriz Procesos vs. Servicios, se asigna un valor de dependencia (Alto, Medio, Bajo).

Para el factor (c), se trabaja con las áreas de impacto y valores de RTO consignados en las Tabla 6, asignándose los valores de impacto (con base en la Tabla 2) para cada una de las áreas. Este factor resulta de la sumatoria del producto del peso relativo de cada área por el impacto acumulado correspondiente.

Áreas de Impacto										
N°	**Áreas**							**Peso Relativo**		
1	Objetivo Estratégicos / Funciones							30%		
2	Financiero							20%		
3	Objetivo y Metas del Proceso u otros Procesos Vinculados							10%		
4	Reputación / Imagen / Credibilidad							30%		
5	Situación y Bienestar del Personal							10%		
	1	2	3	4	5	6	7	8	9	10
RTO	**TR**	**10'**	**30'**	**1 h**	**2 h**	**4 h**	**8 h**	**2 d**	**5 d**	**15 d**
Impacto										

Tabla 6. Áreas de impacto y RTO. Fuente: Elaboración propia.

3.2. Determinación de la probabilidad

Esta labor se realiza con el formato de trabajo ilustrado en la Figura 6, con base en el juicio experto del equipo. Sabiendo la probabilidad de una amenaza se decide qué medidas establecer para reducirlas, medidas que conllevan un coste [10]. La información obtenida en la identificación y la documentación de vulnerabilidades, incidentes y seguimiento de riesgos.

Formato de Análisis de Riesgos de Activos TI

Activo TI	CER		Tipo	Locales / Instalaciones	30-06-11
Administrador			Alterno		
Impacto	5	Mayor	Ubicación	CER	

Tipo	Código	Amenazas de los Activos TI	Exposición / Vulnerabilidad	Riesgo Actual					Control recomendado	Riesgo Residual				
							1	Bajo					1	Bajo
				Frecuencia (F)		NR	R	Riesgo		Frecuencia (F')		NR'	R'	Riesgo
Ataques intencionados	A07	Uso no previsto para sus fines		Raro	1	5	1	Bajo		Raro	1	5	1	Bajo
	A26	Ataque destructivo		Raro	1	5	1	Bajo		Raro	1	5	1	Bajo
	A27	Ocupación enemiga		Raro	1	5	1	Bajo		Raro	1	5	1	Bajo
Desastres Naturales	N01	Fuego		Raro	1	5	1	Bajo		Raro	1	5	1	Bajo
	N02	Daños por agua		Raro	1	5	1	Bajo		Raro	1	5	1	Bajo
	N03	Desastres naturales: Terremotos	Zona sísmica y pronóstico de proximidad	Baja	3	15	2	Medio	Reubicar centro de contingencia en lugar asísmico o distante de Lima (más de 500Km)	Raro	1	5	1	Bajo
	N04	Desastres naturales: Rayo		Raro	1	5	1	Bajo		Raro	1	5	1	Bajo
	N05	Desastres naturales: Tormenta Eléctrica		Raro	1	5	1	Bajo		Raro	1	5	1	Bajo
Industrial	I01	Fuego	Instalaciones eléctricas	Muy Baja	2	10	2	Medio	Mantenimiento permanente de mecanismos correspondientes	Raro	1	5	1	Bajo
	I02	Daños por agua		Raro	1	5	1	Bajo		Raro	1	5	1	Bajo
	I11	Emanaciones electromagnéticas		Raro	1	5	1	Bajo		Raro	1	5	1	Bajo

Figura 6. Formato de análisis de riesgos de activos TI. Fuente: Elaboración propia.

4. Evaluación de riesgos

Con base en los resultados obtenidos en el análisis y la política de aceptación / tolerancia al riesgo, se procede a la evaluación. Para cada activo, si el nivel de riesgo es aceptable, el proceso concluye, caso contrario, se define la estrategia de tratamiento (evitar, transferir o mitigar) y se establecen los controles (salvaguardas) necesarios, pero los mismos no aseguran que el nivel de riesgo sea mínimo. La ejecución de simulaciones permite conocer el estado real de la implementación de los controles [11]. En el caso de mitigación, los controles pueden ser preventivos o correctivos, en el último caso, será necesario definir un Plan de Continuidad de Servicios TI (denominado tradicionalmente PRD - Plan de Recuperación ante Desastres). En esta actividad se concluye el Informe de Análisis de riesgos de activos de información, a partir del cual se elabora el Plan de Tratamiento de Riesgos (PTR).

5. Discusión de la Propuesta

El proceso establece una secuencia metódica para realizar exitosamente el Análisis de Riesgos de activos de información. Éste ha sido elaborado bajo las directrices de estándares y buenas prácticas en gestión de riesgos y seguridad de la información, especialmente MAGERIT.

La diferencia entre la propuesta y dichos estándares se centra en que el proceso explica de manera detallada cómo realizar el análisis de riesgos (no sólo qué se debe hacer), y éste viene siendo aplicado en una institución pública, observándose resultados favorables consistente en la obtención oportuna del "Informe de Análisis de Riesgos de Activos de Información", a partir del cual se elabora el Plan de Tratamiento de Riesgos (PTR) para su posterior ejecución y seguimiento.

Es importante precisar que la diferencia principal con MAGERIT radica en la determinación del impacto, que en este caso se realiza a través del proceso "Business Impact Analysis, BIA", lo cual permite establecer una relación directa entre los activos TI y los procesos institucionales, quienes son los que en realidad causan el impacto en el cumplimiento de la misión.

Considerando que este proceso puede tornarse laborioso cuando se tiene una cantidad relevante de activos (más de 500), se estimó conveniente el diseño y desarrollo de un software de análisis de riesgos, el que forma parte del proyecto "Una Herramienta Peruana para la Gestión del Riesgo Operacional y Tecnológico", cuyo objetivo es contribuir a la generación de ventajas competitivas en las organizaciones.

La idea de la elaboración del software yace sobre el concepto de soporte al proceso propuesto mediante la automatización de puntos operativos del proceso y proporcionando información relevante al especialista en riesgos, la misma que se sintetiza en un mapa de riesgos de activos de información.

Esta herramienta se viene desarrollando con tecnología Java EE bajo una arquitectura distribuida.

El componente que asiste al proceso de análisis de riesgos presentado está constituido por los módulos:

a) Catálogo:

   Facilita la gestión de la información sobre los procesos, los servicios TI que los asisten y los activos TI que constituyen dichos servicios permitiendo la generación de reportes y consultas de dicha información.

b) Análisis de impacto:

   Asiste al subproceso de Análisis Impacto al Negocio (BIA) facilitando la solución de cuestionarios en línea, a partir de los cuales se determina el impacto de los procesos en el negocio y la criticidad de los servicios TI.

c) Análisis de riesgos:

Asiste al subproceso de análisis de riesgos de activos de información donde el especialista de TI asignado para el análisis de riesgos del activo, registra en línea su evaluación en el sistema a través de una interface de usuario. Con esta información se realiza la determinación del nivel de riesgo y se genera el "Informe de análisis de riesgos".

Tal como se mencionó en la introducción del artículo, la concepción del proceso responde a la necesidad creciente de las Organizaciones de implementar proyectos de Seguridad de Información en los cuales **la actividad de Análisis de riesgos es fundamental** y dónde la participación de la alta dirección es determinante, por consiguiente el inicio de un programa de sensibilización a través de la difusión de documentación relacionada se constituye de vital importancia, por ende **el proceso propuesto se complementa con un portal [12] para facilitar sensibilizar e involucrar a todos los miembros de la Organización mediante publicaciones periódicas en materia de Gestión de riesgos y seguridad de información.**

6. Conclusiones

El número de implantaciones de SGSI alineados al estándar ISO 27001 en el país es muy bajo, y más aún las empresas que han alcanzado la certificación. Los pocos proyectos en el rubro tienden a fracasar usualmente debido a la falta de patrocinio, poca conciencia en seguridad de la información y adopción de estándares.

El artículo pretende reducir esta brecha dando los lineamientos generales para abordar un proyecto SGSI, y tratando en detalle el proceso clave de **análisis de riesgos**.

El **proceso propuesto** ha sido aplicado en una entidad pública obteniéndose resultados satisfactorios, lo cual nos permite inferir que el proceso en mención es factible de aplicarse en las demás organizaciones del sector, en un contexto donde existe la necesidad cada vez mayor de implantar un SGSI.

El proceso manual o asistido con herramientas de ofimática puede tornarse engorroso para un número considerable de activos (más de 500). Frente a esta situación y considerando que las herramientas para este fin son escasas y costosas, se ha iniciado el desarrollo de un software.

La conducción de proyectos de implantación de SGSI requiere de facilitadores, los que no están disponibles o están fuera del alcance del presupuesto de nuestras empresas e instituciones. Con el proceso propuesto y la documentación divulgada a través del portal [12] se pretende prestar cierta ayuda.

Referencias bibliográficas

[1]. José M. Huidobro Moya, David Roldán Martínez; "Seguridad en redes y sistemas informáticos" editorial, Thomson Paraninfo, Madrid 2005.

[2]. ISO27000.es: Portal de ISO 27001 en español.

[3]. Alberto G. Alexander; "Diseño y Gestión de un sistema de Seguridad de Información, óptica ISO 27001:2005, editorial: Alfaomega, 2007.

[4]. Presidencia del Consejo de Ministros (PCM/ ONGEI), Resolución Ministerial N° 129-2012-PCM

[5]. Bilge Karabacaka, Ibrahim Sogukpinarb; "ISRAM: information security risk analysis method", National Research Institute of Electronics & Cryptology (UEKAE), P.O Box 74, 41470 Gebze, Kocaeli, Turkey; Gebze Institute of Technology, 41400 Gebze, Kocaeli, Turkey; July 2004.

[6]. AS/NZS 4360:2004. Estándar Australiano / Neozelandés para la gestión de riesgos.

[7]. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas – MAGERIT.

[8]. NIST - Risk Management Guide.

[9]. Eduardo Fernández, Medina Patón; Roberto, Moya Quiles, "Seguridad de las tecnologías de información", Construcción de la confianza para una sociedad conectada. Editorial: AENOR, Madrid, 2003.

[10]. Vicente Aceituno Canal; "Seguridad de la información, Expectativas, Riesgos y Técnicas de protección", Editorial Limusa, México 2006.

[11]. Pedro Andrés, Morales Zamudio; Diseño de una solución de un sistema de seguridad informática en empresas estatales, Informe de Suficiencia profesional, Lima, 2010.

[12]. Portal de difusión de la documentación del Proceso propuesto y de Seguridad de Información, www.EmprendedorTIC.net/sgsi